



COMMUNITY DAY

AOTEAROA

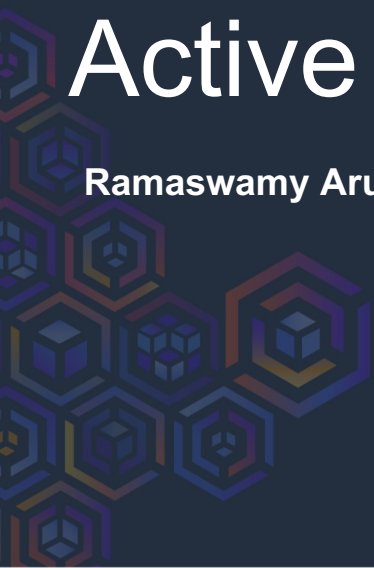


COMMUNITY DAY

AOTEAROA

Active Directory DS in AWS

Ramaswamy Arunachalam | 06-Sep-2023





COMMUNITY DAY

AOTEAROA

My Intro

- Based out of Wellington
- Solution Architect
- Passionate About:
🏏 Cricket | 🏎️ F1 | 🦹‍♂️ Superhero Movies | 🐕 Dog Lover.



Why Active directory is essential in AWS Universe?

- Ensure consistent user experience in Hybrid environment.
- Support Windows work load with authentication.
- Integrate with AWS applications & services.
- High speed, reliable & low latency to applications.

AD deployment Options in AWS

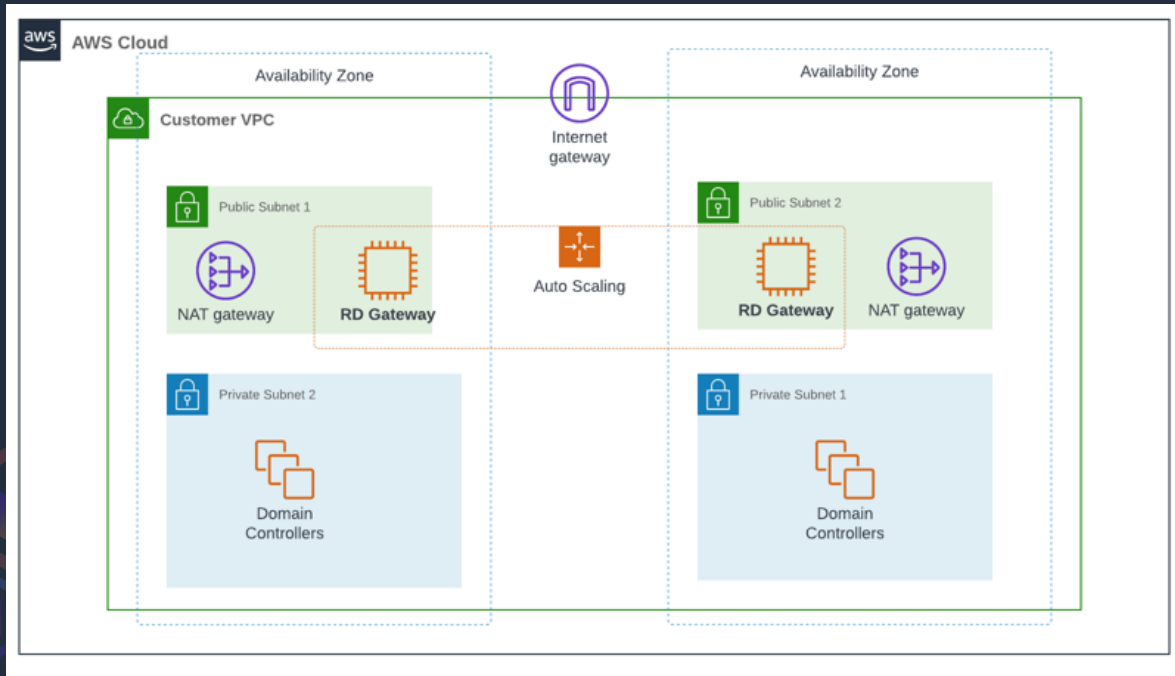


- We can choose Self-Managed AD when
- Extend existing on-premise Domain/Forest to AWS.
 - Integrated environment - on-prem and AWS.
 - Requirement of Domain Admin privilege.
 - Utilization of existing users, groups, OU and GPOs



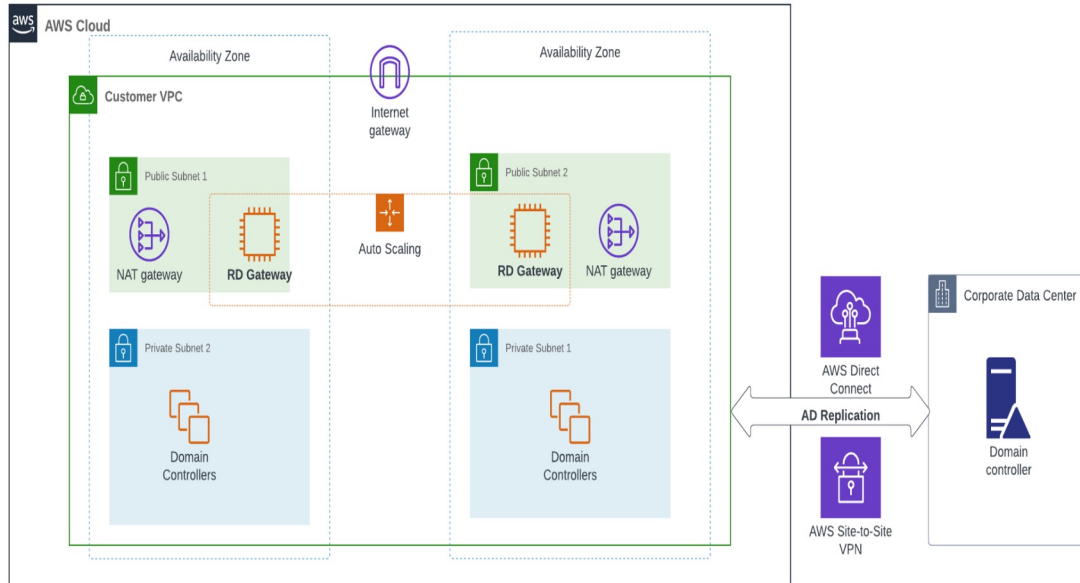
- We can choose AWS Managed AD when
- Isolated Domain for AWS resources.
 - Minimize operational over-head of AD Infrastructure.
 - Delegate cloud AD Management to separate team while maintaining control of users identity.
 - Requirement of AWS-native authentication.

Self Managed Active Directory



aws
COMMUNITY DAY
AOTEAROA

Self Managed Active Directory Extended to AWS

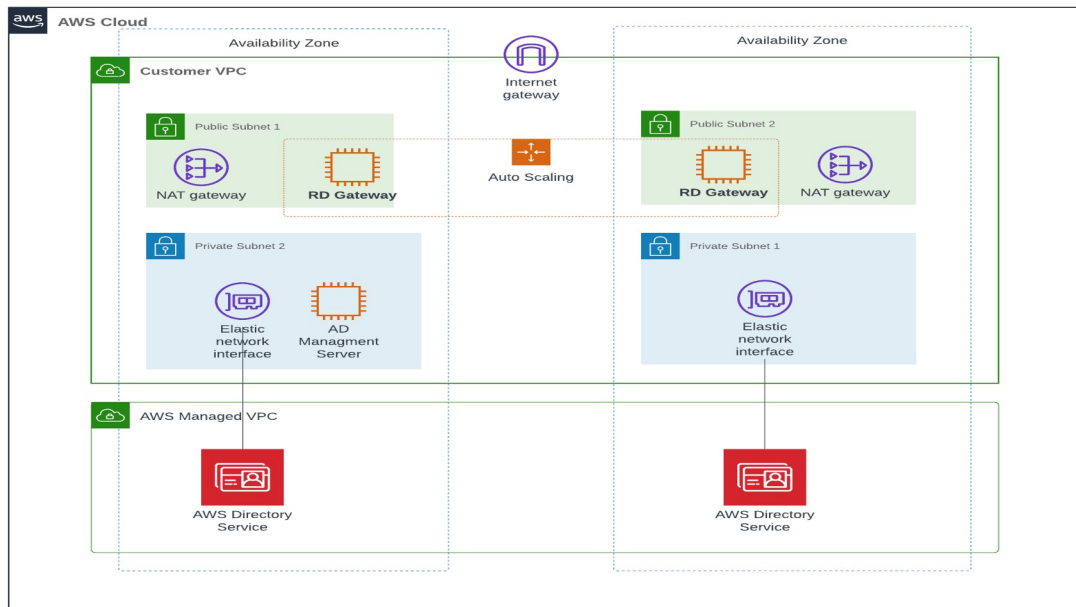




Working on updates 0% complete.
Don't turn off your PC. This will take a while.

Your PC will restart several times.

AWS Managed Active Directory



- Powered by Windows 2019 and operates at Windows 2012 R2 Forest and Domain functional level.
- Minimum two subnets and both in different Availability Zone.
- VPC with default hardware tenancy.
- AWS Managed Microsoft AD can't be created in a VPC using addresses in the 198.18.0.0/15 address space.
- Single directory sharing with other AWS accounts within same or outside organization.

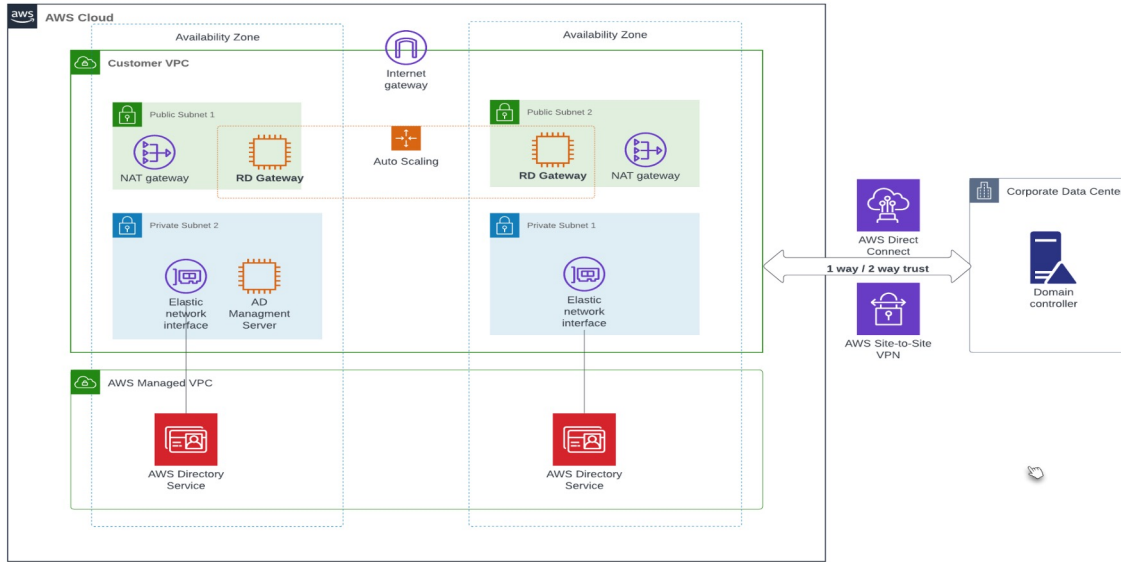




COMMUNITY DAY

AOTEAROA

AWS Managed AD Trust On-Premises AD

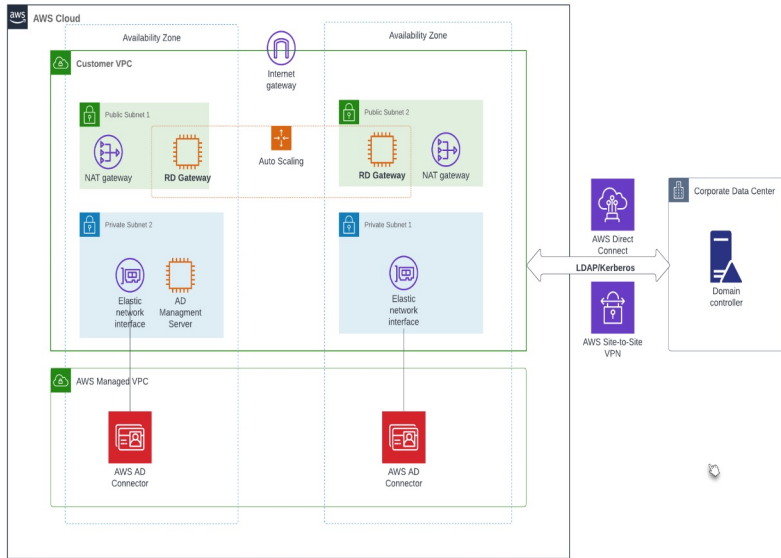




COMMUNITY DAY

AOTEAROA

AWS AD Connector - On-Premises AD

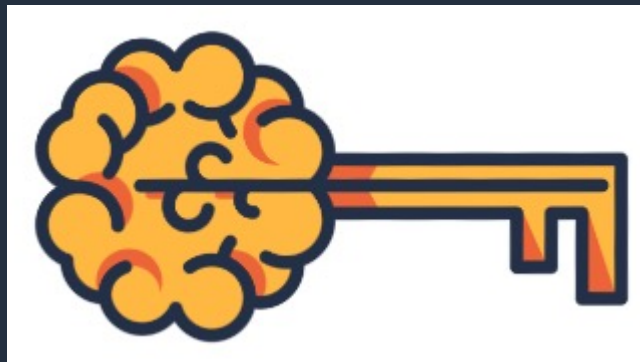


- Directory gateway – redirect to On Prem AD
- No caching in cloud
- Two sizes small and large
- AD Connectors works only with AWS applications.
- No support for AD Transitive trusts.
- AD Connectors cannot be shared with other AWS accounts and needs 1 to 1 relationship with on-prem



Key Takeaways – AD in AWS

1. Seamless Hybrid Identity Management
2. Scalability and Availability
3. Security and Compliance





COMMUNITY DAY

AOTEAROA



Let's Network! Find me on LinkedIn

@

<https://www.linkedin.com/in/ramstack/>



References

For more information on Active Directory DS in AWS, please refer the following links

- <https://aws.amazon.com/solutions/partners/active-directory-ds/>
- https://www.youtube.com/watch?v=j1Fhaeh_MFA



COMMUNITY DAY

AOTEAROA